

NIS-2 GAP Analyse und kontinuierliche Verbesserung mit GAP View Software

1. Einführung

Die zunehmende Digitalisierung aller Lebens- und Arbeitsbereiche einerseits und die steigenden Cyberbedrohungen andererseits machen eine robuste und flächendeckende Cybersicherheitsstrategie unerlässlich. Mit der NIS-2-Richtlinie (*Network and Information Security Directive 2*) verfolgt die Europäische Union das Ziel, das gemeinsame Sicherheitsniveau im Bereich der Netz- und Informationssysteme deutlich zu verbessern. Die nationale Umsetzung dieser Richtlinie ist daher ein entscheidender Schritt, um die digitale Souveränität und Resilienz Deutschlands nachhaltig zu stärken. Sie ist im „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)“ festgelegt. Das NIS-2-Umsetzungsgesetz ist seit dem 6. Dezember 2025 wirksam und betrifft einen erheblichen Teil der deutschen Wirtschaft mit mehr als 30.000 Unternehmen.

2. Wer ist betroffen?

Der Geltungsbereich des NIS-2-Umsetzungsgesetzes geht weit über den bisher bekannten Kreis der KRITIS-Unternehmen hinaus. Direkt betroffen sind sogenannte „besonders wichtige Einrichtungen (bwE)“ und „wichtige Einrichtungen (wE)“ (vgl. §§ 28 und 29 BSIg). Neben der Zugehörigkeit zu einem Wirtschaftssektor oder einer Branche sind die Anzahl der beschäftigten Mitarbeiter, der Jahresumsatz und die Bilanz von Bedeutung. Betroffen sind Unternehmen mit mehr als 50 Mitarbeitern, einem Umsatz von mehr als 10 Mio. Euro und einer Bilanzsumme von mehr als 10 Mio. Euro. Dazu zählen Anbieter von Waren und Dienstleistungen aus den Bereichen Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur, Weltraum, Post- und Kurierdienste, Abfallwirtschaft, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln sowie des verarbeitenden Gewerbes/der Herstellung von Waren und der Forschung. Darüber hinaus zählen dazu Anbieter öffentlich zugänglicher Telekommunikations-

dienste oder Betreiber öffentlicher Telekommunikationsnetze sowie Vertrauensdiensteanbieter, Top-Level-Domain-Namen-Registry oder Anbieter von DNS-Diensten.

3. Gesetzliche Pflichten der betroffenen Unternehmen (Auszug)

- **[§ 38]** Die Geschäftsleitung von „besonders wichtigen Einrichtungen (bwE)“ und „wichtigen Einrichtungen (wE)“ sind verpflichtet, die Risikomanagementmaßnahmen gemäß § 30 umzusetzen und deren Umsetzung zu überwachen.
- **[§ 33]** Die betroffenen Unternehmen müssen sich spätestens bis zum 6. März 2026 über ein zentrales Portal bei dem Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren.
- **[§ 30]** Es müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen umgesetzt werden, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden, zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Darunter:
 - Risikoanalyse und Sicherheitskonzept
 - Bewältigung von Sicherheitsvorfällen
 - Betriebliches Kontinuitäts- und Krisenmanagement
 - Sicherheit von Lieferketten
 - Sicherheit in der Beschaffungs-, Entwicklungs- und Wartungsphase
 - Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik
 - Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik
 - Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren
 - Personalsicherheit, Zugriffskontrolle und Verwaltung von IKT- Systemen, -Produkten und -Prozessen
 - Multi-Faktor-Authentifizierung, kontinuierliche Authentifizierung, gesicherte Kommunikation

- **[§ 32]** Bei festgestellten Sicherheitsvorfällen besteht Meldepflicht innerhalb vorgegebener Fristen.
- **[§ 38]** Die Geschäftsleitung ist verpflichtet, regelmäßig an Schulungen teilzunehmen, um ausreichende Kenntnisse zur Erkennung und Bewertung von Risiken im Bereich der Informationssicherheit sowie deren Auswirkungen zu erlangen.

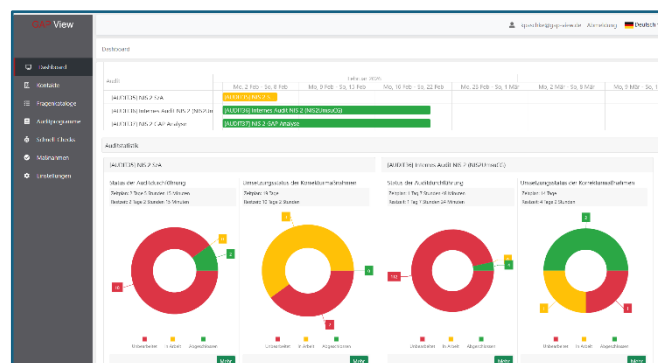
4. NIS-2 Roadmap

Die vom BSI veröffentlichte NIS-2-Roadmap zeigt eine systematische Vorgehensweise (Phasen) für die Umsetzung der Richtlinie auf. In zwei dieser Phasen kommt die Audit-Management-Software GAP View zum Einsatz. Einerseits bei der Feststellung des aktuellen Standes der Cybersicherheit (Gap-Analyse), andererseits bei der kontinuierlichen Verbesserung der umgesetzten Sicherheitsmaßnahmen (kontinuierliches Monitoring).

5. Gap-Analyse mit GAP View Software

Mithilfe der GAP View Software und des bereitgestellten Fragenkatalogs kann der aktuelle technische, organisatorische und prozessuale IST-Zustand der Cybersicherheit im Unternehmen ermittelt werden. Der speziell dafür entwickelte detaillierte Fragenkatalog basiert auf dem Mapping der ISO/IEC 27001 Controls auf die NIS-2-Sicherheitsanforderungen (NIS2UmsuCG). Die auf diese Art und Weise ermittelten Abweichungen (GAPs) zwischen den NIS-2-Sicherheitsanforderungen und dem vorgefundenen IST-Zustand werden in einem automatisch erstellten Maßnahmenkatalog zusammengefasst. Im Maßnahmenkatalog können Verantwortlichkeiten, Umsetzungshinweise, Prioritäten, Zeitaufwand und Fristen für die Umsetzung festgelegt werden. Bei der Konzeption der Umsetzungshinweise kann über eine integrierte Schnittstelle direkt auf OpenAI ChatGPT zugegriffen werden. Der Maßnahmenkatalog stellt somit eine Grundlage für die Planung der Umsetzung von NIS-2-Sicherheitsanforderungen dar. Durch die regelmäßige Aktualisierung des Umsetzungsstatus (Dashboard und Bewertung) einzelner Sicherheitsmaßnahmen und die

Generierung entsprechender Berichte können die Geschäftsleitung und beteiligte Mitarbeiter über den Fortschritt im Projekt informiert werden.



6. Kontinuierliche Überwachung mit GAP View Software

Die Überwachung der umgesetzten Sicherheitsanforderungen erfolgt in der Regel im Rahmen von internen und externen Audits. Die GAP View Software wurde speziell für die effiziente, kontinuierliche Überprüfung der Wirksamkeit, Vollständigkeit und Angemessenheit von Managementsystemen für Informationssicherheit entwickelt und ist somit sehr gut für die Erfüllung der Anforderungen gemäß § 38 NIS2UmsuCG geeignet. Sie bildet die Anforderungen an die Planung und Durchführung von internen und externen Audits nach ISO 19011 und ISO/IEC 17021 sowie IS-Revisionen gemäß dem BSI-Leitfaden „IS-Revision auf Basis von IT-Grundschutz“ und dem Baustein DER.3.1 „Audits und Revisionen“ ab.

7. GAP View Software - Weiterführende Informationen und Webinare

Über NIS-2-Gap-Analyse und Umsetzung der kontinuierlichen Überwachung nach § 38 NIS2UmsuCG finden Sie unter

<https://www.gap-view.de/>

und

<https://www.gap-view.de/Webinare.html>